# PROFESSIONAL SERVICES

Creating Sustainable Business Advantage


# PKI Assessment Document

**5 June 2000**

*Prepared for:*
**Ken Adrian**
**State of Iowa, IT Department**
**ITS 'B' Level, Hoover Building**
**Des Moines, IA 50319**

*Prepared by:*
**Professional Services**
**10 Fawcett Street**
**Cambridge, MA 02138**

# Table of Contents

1.0 Executive Summary ..... 3
1.1 Purpose ..... 3
1.2 Main Points ..... 3

2.0 Overview ..... 4
2.1 Purpose of Document ..... 4
2.2 Intended Audience ..... 4

3.0 PKI Technology Overview ..... 4
3.1 Overview ..... 4
3.2 Needs Assessment Methodology ..... 5

4.0 State of Iowa PKI Plans ..... 6
4.1 State PKI Responsibilities ..... 6
4.2 State PKI Functions ..... 6
4.3 Phase-in of Services ..... 6
4.4 PKI Provider Models ..... 6

5.0 Current PKI Enabled Applications ..... 8
5.1 What Can Be PKI-Enabled ..... 8
5.2 Access Control ..... 8
5.3 Secure E-mail ..... 10
5.4 SSL (Browser and Server PKI) ..... 10
5.5 Virtual Private Networks ..... 11
5.6 Electronic Form Signing ..... 12
5.7 Desk Top File Encryption ..... 13
5.8 Wireless Applications (WAP TSL) ..... 13
5.9 Document Transfer (EDI) ..... 14
5.10 SET ..... 14

6.0 Summary of Requirements from Interviews ..... 16
6.1 Overview ..... 16
6.2 Possible PKI-enabled Applications ..... 16
6.3 Number of Certificates ..... 18
6.4 Trust Hierarchy ..... 18
6.5 Roots ..... 19
6.6 Certificate Period and Renewal ..... 19
6.7 Certificate Revocation ..... 20
6.8 Encryption Certificates ..... 20
6.9 Communica-tions Capacity ..... 21
6.10 Reports ..... 21
6.11 Billing ..... 21
6.12 Help Desk ..... 21
6.13 Backup Facility ..... 22

7.0 Certificate Types and Content ..... 23
7.1 Types of Certificates ..... 23
7.2 Certificate Contents ..... 23

8.0 Registration Processes ..... 25
8.1 Levels of Authentication ..... 25
8.2 Manual Authentication ..... 25
8.3 Automated Authentication Methods ..... 26
8.4 Authentica-tion Criteria ..... 26
8.5 Who Performs Face-to-Face Authentication ..... 27
8.6 Who Performs RA Functions ..... 27
8.7 PKI Kiosks ..... 27
8.8 Biometrics ..... 28
8.9 Data Sensitivity ..... 28

9.0 CA Hosting Facility ..... 29
9.1 Facility Overview ..... 29
9.2 CA Facility Security Requirements ..... 29
9.2.1 Introduction ..... 29
9.2.2 Site Physical Security ..... 29
9.2.3 Facility Operational Controls ..... 30
9.3 CA Facility Staff ..... 31
9.3.1 Required Personnel ..... 31
9.3.2 Staff and Responsibilities ..... 31
9.3.3 Officers ..... 31
9.3.4 Facility Manager ..... 32
9.3.5 Site Security Officer ..... 32
9.3.6 Data Base Administrator ..... 33
9.3.7 Site Administrators ..... 33
9.3.8 Online Operators ..... 33
9.3.9 RA Operator ..... 34
9.3.10 Security Functions ..... 34
9.3.11 Staff Assignments ..... 34

Appendix 1 Agency Staff Interviewed and Possible Applications ..... 35

Appendix 2 Sample Certificate Format ..... 38

References ..... 40
40

## 1.0 Executive Summary

### 1.1 Purpose

The purpose of this document is to identify requirements for a Public Key Infrastructure (PKI) implementation for the State of Iowa, based on interviews and documentation provided by State agencies. A new Iowa law requires that most State business that now requires physical signatures must be offered on-line using digital signatures. The state Information Technology Department (ITD) has been tasked with providing the necessary infrastructure. The requirements from this document will in turn provide input for follow-on documents: a proposed architecture, a vendor survey, and a cost analysis. Additionally, a review of a proposed CA facility, to be used if Iowa decides to run their own Certification Authority, was conducted and additional physical security requirements were identified.

### 1.2 Main Points

- This document summarizes expected requirements for a State of Iowa PKI, based on interviews with State agency staff, experience of Baltimore Technologies consultants, and PKI industry standards.
- A brief survey of public key technology is included in section 3.
- The State has yet to decide whether to run its own certification authority (CA) or outsource this function to a commercial service vendor.
- State agencies assume that a main use of the PKI, including CA and applications, will be to control web-based access to State backend databases for citizens and government employees. This is a result of the new State law requiring Internet access with digital signatures (which implies a PKI with digital certificates and a certification authority) by 1 July 2003 for most State systems that presently require face-to-face paper-based processes with handwritten signatures.
- Other applications that may be protected via the PKI, if warranted in the judgement of the respective agencies, include:
    - Secure e-mail
    - Secure web browser and server connections
    - Virtual Private Network (VPN) remote access systems
    - Form signing and file encryption
    - Wireless applications
    - EDI, XML and other business applications
- The expected number of certificates is uncertain at this time. A guideline is that it would be prudent to plan for a few systems of 10,000 users or less in the next two years, and several systems of 100,000 or more after mid-2003.
- It is presumed that the State of Iowa will have its own Root CA. The State may also be interested in having its Root signed by a commercial Root embedded in major applications (browsers, servers, e-mail packages) to simplify user interfaces, or in cross-certifying with other state or federal peers.
- Various State agencies have different ideas on who should perform the certificate authorization (request approval) process, and run help desks. A flexible design to cover all options is suggested. This should include at least three choices for the identification method.
- Due to the State's client-server environment, it is suggested that certificates can be simple, multi-application, and relatively long-lived (multi-year) in most cases.
- Requirements for running a CA, whether performed by the State or a service vendor, are summarized.

## 2.0 Overview

### 2.1 Purpose of Document

The purpose of this document is to present the needs of the State of Iowa with respect to a Public Key Infrastructure (PKI) and Trusted Third Party (TTP) services. The document summarizes the requirements that must be met to conform to known applicable laws, standards, and Iowa's strategic objectives. This document provides the basis for a proposed architecture, and the actual PKI architecture document to be delivered later in this engagement describes a baseline certification system design in detail.

### 2.2 Intended Audience

This document is intended for the use of technical staff and managers of the State government, to assist planning and implementing a PKI within the State of Iowa.

## 3.0 PKI Technology Overview

### 3.1 PKI Overview

*"Public key technology depends upon complicated mathematical concepts but it has a simple, understandable effect: When an individual (we will call him "Bob") starts to participate in the PKI, he begins with a pair of "keys," which look like very long character* [or binary] *strings and are actually digital representations of very large numbers. These keys are either chosen by Bob or provided through trustworthy mechanisms, subject to certain mathematical requirements. One of these keys is secret (private) and the other is published (public).*

*The essence of public key technology is that messages or transactions authenticated or encrypted using one of Bob's keys can only be verified or decrypted using his other key. Thus, when Bob uses his private key to sign an electronic message or other transaction digitally, anyone who knows Bob's corresponding public key can verify Bob's signature. A similar method using public key technology can be used to encrypt messages for confidentiality, and then decrypt them.* [In the latter case, the recipient's public key is used for encryption and the recipient's private key is used for decryption.]

*The evolving PKI will use special digitally signed documents (called "certificates") to bind Bob's identity to his public keys. Digital certificates are provided by a trusted "Certification Authority" (CA) and signed using that CA's private key.* [Virtually all certificates used today follow the ISO X.509 standard.] *When someone else (we will call her "Alice") wants to obtain with certainty Bob's public key, she may get Bob's certificate from Bob in person, or she may get it from an on-line "repository" for certificates, or even from Bob's homepage on the World Wide Web. Where or how Alice gets Bob's certificate is not important, because she validates the certificate by validating the CA's digital signature. Alice now knows Bob's public key and name with certainty and can validate any messages sent to her which were signed with Bob's private key. These transactions may be conducted with assurance even though Bob and Alice may never have met.*

*To validate the CA's signature on Bob's certificate, Alice must first know the public key of Bob's CA. Alice only needs to know public key of the one CA that she trusts. CAs may issue certificates to each other. If Alice does not know the public key of Bob's CA, she can find a certificate issued by a CA whose key she does know, that will certify the public key of Bob's CA. Much of the challenge of building a robust global PKI is in the management of certificates among CAs, as well as the software and infrastructure that automate the process of building and validating these trust chains of certificates. A Model Certificate Policy document for Federal government use is being prepared to promote this process…* [The other major challenge is ensuring that the CA has the information needed to be sure the data in users' certificates is valid before issuing them.]

*As a general matter, good security practices will permit and encourage Bob to have different public-private key pairs for signature and confidentiality uses, and to reflect his different roles (e.g., as an agency official, and as a private citizen and consumer). This is analogous to a person having different passwords for use on different computer systems, or different PINs for use with different financial accounts.*

*The scientific, academic, and business communities recognize that the capabilities described above provide the best way to replace handwritten signatures in the electronic world, to authenticate identities securely, and to maintain confidentiality on open networks.*

*To realize this vision of transacting electronic business with security and privacy, it is critical that the various implementations of public key technologies work together smoothly and in a fashion transparent to the user. Neither Bob or Alice should have to study cryptography to use the technology with comfort and ease!"*

*-- Access with Trust, September 1998, 14-16*

[with comments added for this document]

### 3.2 Needs Assessment Methodology

This report documents the information gathered during a Needs Assessment conducted in state government offices at Des Moines between 22 and 26 May 2000. The Assessment was done on behalf of the State of Iowa, coordinated via the state Information Technology Department (ITD). Several interviews were conducted with key representatives from several agencies in the Executive branch, starting with ITD, and one interview with Legislature staffers in case they decide to participate as well. The interviews identified needs, requirements and ideas for possible uses of the PKI.

## 4.0 State of Iowa PKI Plans

### 4.1 State PKI Responsibilities

Given the cost of creating a PKI, CA security requirements, continuing operations cost and staffing requirements (both numbers and skills set), most state agencies could not realistically install a PKI with a Certification Authority. The likeliest solution is for a central organization to become a Trusted Third party and provide PKI services to the state agencies. It has not yet been decided whether this service will be provided by a state agency (presumably ITD) using equipment and software purchased from vendors, or will be outsourced to a commercial company provides such services. This requirements analysis and following documents will help the State of Iowa make this decision.

### 4.2 State PKI Functions

State agencies, assisted by ITD, offers a variety of communication services to the public and/or to state government employees. These presently include access to state servers and data banks to provide services to citizens, e-mail and web access, and remote access for traveling government employees. PKI-based systems are thus likely to include secure (via certificates) access to servers, secure email and web (browser) access, Virtual Private Network (VPN), Wireless Access Protocol (WAP) for accessing the Internet via mobile phones, and web hosting, among others. It is important to examine those services and determine how PKI can best be integrated into these offerings.

### 4.3 Phase-in of Services

The scope for the use of digital certificates within state government could initially be relatively small, with initial target areas being designated agencies, users within those agencies, and citizens using those agencies' services. This would allow ITD to gain experience with running or subcontracting a CA in a relatively non-stressed environment. Once a CA and the associated infrastructure is available to government and has proven its usefulness, there will be opportunities to involve greater numbers of both government employees and the civil population. There is generally a recognitiion of the need for government to be seen as leading and supporting the use of this technology and actively promoting secure electronic services to replace traditional paper and physical signature based business models.

### 4.4 PKI Provider Models

There are two distinct models for providing state PKI services: in-state hosting or outsourcing. In boths case there are at least two levels of CAs. A Root CA contains a very carefully guarded private key that is used only to sign certificates provided to subordinate CAs. The Root CA is normally kept off-line, not connected to any network, and is activated only when a subordinate CA is initialized or updated, or when a CA (not user) certificate revocation list must be prepared. The public key of the Root CA, contained in a self-signed certificate, is distributed to applications that must trust that CA. Subordinate CAs are connected to a network, typically the Internet, and provide certificates to end-users and certificate revocation lists to applications that must rely on those certificates.

The in-state hosting approach is for a state agency to actually run a CA. ITD is the obvious candidate in this case. ITD would build or adapt a secure facility suitable

for hosting a CA, purchase standard computer hardware and software, and purchase and install CA software from a vendor. ITD would then run the CA on behalf of state agencies. It is simplest to have all CAs, including a State of Iowa offline Root CA used only to set up other CAs and other infrequent functions, and operational on-line subordinate CAs that perform the day-to-day PKI functions, in one location. As users access the CA via the Internet or similar network, they would not normally know or care exactly where the subordinate CA is located, so centralization in one facility is practical. An agency can have its own subordinate CA that is specialized for that agency's operational and data requirements, or can share a subordinate CA with other agencies that have similar PKI requirements. Some agencies might choose to run their own subordinate CA if they have secure-enough facilities, for example Iowa State University might have the capability.

The outsourcing approach may make sense if the state government decides after analysis that it does not wish to purchase and operate a CA itself. In this case, the state can contract with a commercial CA to add a State of Iowa Root CA and subordinate CAs. These CAs, or at least the on-line subordinate CAs, would be operated out of an existing secure facility. This facility is likely to be outside Iowa, although users may not be aware of this. The State of Iowa can still retain control of the State Root CA, if it wishes, by maintaining physical control of the cryptographic unit with the Root private key.

## 5.0 Current PKI Enabled Applications

### 5.1 What Can Be PKI-Enabled

This section summarizes some PKI-enabled applications that may be of interest to the State of Iowa. Reactions of interviewees

The PKI is a secure system storing information about users and devices in the form of digital certificates. Digital certificates are signed by a trusted authority that provides confirmation that the certificate positively identifies the certificate presenter. Certification Authorities (CAs) act as agents of trust in a PKI. CAs represent the people and processes which create digital certificates that securely bind the names of users to their public keys. As long as the user community trusts a CA and its operational policies for issuing and managing certificates, they can trust certificates issued by the CA. This is referred to as third-party trust.

PKI is strategically important not only for corporate users of the service, but for suppliers of e-commerce services. The "proof of identity" responsibility performed by a CA can be passed to a third-party organization so that secure e-commerce can be transacted. The PKI provides the framework for building global trust for e-business.

However the realization of certificate issuance alone does not provide the organization with the benefits of strong security. The value of security technologies rests with the applications that leverage the PKI. To date a number of applications have achieved these gains and are being actively incorporated into secure business solutions. These applications are defined to be PKI enabled, as well as any other application that uses this technology to secure it.

### 5.2 Access Control

Virtually all agencies that were interviewed saw their primary task related to PKI as providing secure access to one or more central back-end servers and associated databases. The new State of Iowa electronic commerce act requires that most state functions that now involve the use of paper and physical signatures must also be offered to the public over the Internet using digital signatures, by 1 July 2003. This means that individuals who are not observed face-to-face by any state employee (except possibly when they request a certificate) must be allowed to access critical data and perhaps modify that data, based on information provided in a certificate. These back-ends are to be accessed remotely via the Internet or other similar network, so it is critical to identify who is accessing the back-ends and ensure that each user is allowed to see or modify only appropriate data.

**What is access control?**

The definition of “access control” includes:

- A process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems in a network) according to a security policy. [SPC recommended definition]
- Protection of system resources against unauthorized access. [SPC alternate recommendation]
- “The prevention of unauthorized use of a resource, including the prevention

of use of a resource in an unauthorized manner." [ISO/IEC 7498-2]

The delivery of effective access control is complex. It requires a combination of security services:

- strong authentication establishes the identity of a user,
- policy management defines the rules to govern what resources the user can access, and
- policy enforcement implements those rules.

Users and vendors often include additional security services under the umbrella of "access control", including data confidentiality, data integrity, and audit capability.

All of these services must be deployed in a way that is usable and manageable, often in environments that present a heterogeneous mix of hardware architectures, operating systems, networking protocols, and applications. Access control is a complex problem.

**Why is access control important?**

As enterprises take advantage of internetworking technologies to reduce costs and increase opportunities, greater amounts of valuable or sensitive information is being made available to employees, customers, and business partners. For example, organizations are using intranets to deliver confidential personnel information to their employees, and they are using extranets to conduct commerce with customers or suppliers and to collaborate with partners. In each of these scenarios, access control mechanisms play a crucial role, preventing inappropriate – and potentially costly – information exposure by ensuring that users access only the resources for which they are authorized.

**How are digital certificates relevant to access control?**

Authentication is an essential link in the chain of services that constitute an access control solution, and the solution can only be as strong as its weakest link. By enabling strong authentication – and the possibility of multi-factor authentication via smart cards or biometrics – digital certificates can provide a solid foundation for access control. Certificates authenticate users with a high degree of assurance and without the management costs and the risks of misuse that are associated with passwords.

Legal and regulatory considerations are driving some market segments to certificate-based solutions for access control. HCFA (Health Care Financial Administration) regulations, for example, are driving the health care industry and government agencies to use digital certificates to protect access to medical records via the Internet. In any other markets where highly valuable or sensitive information is selectively shared, such as financial services or law enforcement, certificate-based access control solutions are a natural fit.

**5.3 Secure E-mail**

S/MIME is an Internet protocol developed by an industry consortium led by RSA Data Security, Inc. S/MIME requires the use of X.509 certificates to send encrypted e-mail messages and authenticate received messages. Based on a secured version of the popular Internet MIME standard, S/MIME provides the following security services for electronic messaging applications:

- *Authentication* – using X.509 public key certificates
- *Data Confidentiality* – using encryption
- *Data Integrity* – using digital signatures
- *Non-repudiation* – using digital signatures

S/MIME has been chosen by practically every major mail vendor (e.g., Microsoft, Netscape, Novell and IBM) allowing users to choose from a variety of interoperable e-mail solutions. This is because of S/MIME's comparative maturity, ability to provide non-repudiation services, fine granularity on protection of objects (e.g. messages, web pages), support for centralized key management via X.509 certificate servers, and widespread industry support.

While many of the email clients have been PKI enabled, they still do not always interoperate well with each other. When customers are faced with heterogeneous collections of email clients, they may need additional applications, like Baltimore's MailSecure, to make it easier to use.

**5.4 SSL (Browser and Server PKI)**

Secure Sockets Layer (SSL) is an Internet protocol originally developed by Netscape that uses connection-oriented end-to-end encryption to provide the following security services:

- *Authentication* – server authentication (verifying the server's identity to the client) and optional client authentication (verifying the client's identity to the server).
- *Data confidentiality* – for application layer traffic between a client and a server.
- *Data integrity* – for application layer traffic between a client and a server.

SSL is layered below an application protocol (e.g., HTTP, Telnet, or FTP) and above a reliable transport protocol (e.g., TCP). It has two common versions: SSL version 2 (SSLv2) provides only for servers to have certificates and authenticate themselves to users, while SSLv3 provides for both servers and users (browsers) to be certified and authenticate themselves to the other party.

An SSL connection set up has two basic phases:

1. The first phase is the negotiation/authentication phase in which the server and (for SSLv3) client are authenticated to each other. During this phase, the SSL Handshake Protocol allows the two communicating endpoints to agree on the cryptographic and key exchange algorithms.
2. The second phase is the data phase. During this phase, the raw original data

is encapsulated in a simple SSL encapsulation protocol (SSL Record Protocol). (The key material used to protect the data was generated/agreed during the negotiation/authentication phase in step 1.) A temporary one-time encryption key, kept only for this session, is generated to provide data confidentiality.

The main advantage to SSLv3 is that it is independent of the application it encapsulates, and a higher level protocol can layer on top of SSLv3 transparently. A disadvantage to SSL is that it only protects a communication connection (i.e. a "pipe") and not the individual objects communicated over the pipe. Because of this SSLv3 can not provide the non-repudiation service or protect individual objects, for example, web pages. Despite its disadvantage, the SSLv3 protocol is widely deployed over the Internet in the form of SSLv3-capable servers and clients from vendors like Netscape and Microsoft.

The State of Iowa is likely to require both browser certificates for individual end-users to access state servers, and web server certificates for the state's back-end servers. These certificates are obtained via quite different methods, and the CA and PKI system should support both. In general, obtaining a server certificate requires that the server organization be authenticated much more carefully, since large numbers of users will rely on the CA's signature on the server certificate to trust that server.

### 5.5 Virtual Private Networks

Virtual Private Networks (VPN) enable the secure exchange of data across untrusted networks. Almost all VPN products now use IPSec (IP Security), a framework of open standards for ensuring secure private communications over the Internet.

Fundamentally, IPSec protects IP packets during their transmission over an Internet or Intranet whether via intermediary routers, firewalls or end systems. IPSec provides confidentiality, authentication and integrity services. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Authentication Header (AH) allows authentication of the sender of data, and Encapsulating Security Payload (ESP) supports both authentication of the sender and encryption of data as well.

Effective management of the VPN solution is provided through a security architecture based upon PKI. A PKI provides VPN with the benefits of certificate management and validation. When a security association is established via public key, each node communicates with the CA to verify that the other node's certificate is valid. This generally includes checking the certificate against a certificate revocation list (CRL) that is maintained by the CA administrator and made available on a public directory service. Revocation enables an organization to prevent or deny authentication of a certificate belonging to a VPN once it has been determined that the certificate has been compromised in some way and should not be trusted. If the certificate is not deemed valid, an encrypted tunnel may not be established.

Private/public key technology enables strong authentication techniques. Key exchange without the use of trusted certificates received from a PKI or trusted third party is susceptible to attacks, especially the "man in the middle" attack. This attack involves an imposter fooling mutual parties of a connection into performing a key exchange with an attacker and not the intended party (spoofing). The certificates

received from a PKI provide reliable authentication and secure key negotiation by allowing each party to verify that the host that they are communicating with is indeed who they say that they are. A PKI is especially important when setting up a VPN between an organization and its business partners or suppliers because it requires a secure key exchange from a third party CA that is "trusted" by both VPN nodes.

The use of certificates allows the implementation to scale to large networks that require secure connections between many devices. The availability of public key certificates from a public repository eliminates the requirement for laboriously exchanging certificates between each potential end-point in a complex network.

VPN protects the transmission channel and not the objects within the connection. Applications utilizing the secure channel need not participate in establishing the security services. For this reason, integration issues are minimal. IPSec is available as a software-only upgrade to the network infrastructure. This permits VPN security to be implemented without costly changes to every computer or application. This provides great cost-savings because only the network infrastructure needs to be changed.

### 5.6 Electronic Form Signing

The ability to digitally sign electronic forms provides authentication and non-repudiation of employee, customer, and business partner requests. Businesses can utilize electronic form signing to facilitate business process re-engineering efforts. Existing paper-based business processes can be replaced and streamlined with electronic processes that take advantage of form signing and work flow capabilities.

> ***"How secure are E-form digital signatures?*** *The level of security provided by a digital signature is based on the level of trust provided by the signing service and the security maintained on the user's private key that creates the signature. For example, a private key protected by a weak password on an easily compromised PC will create a signature with a very low level of trust. Signing an E-form does not automatically control access to that form. Controls within the E-form application itself, and within the underlying network services, determine access. An electronic or digital signature provides authentication without encrypting the form. While this may be "enough" security for many applications, it is not sufficient for confidential information, such as patient-identifiable records or sensitive law enforcement information.*
>
> *The major IEFM vendors offer digital signature options to secure E-forms at several levels. A potential problem arises when trying to re-create the original form and prove its integrity for a period of time. This is necessary to comply with legal requirements that electronic record documentation be "equivalent to paper." In an IEFM system, each completed form can be stored as two separate files: one with the E-form template, the other with the data, each protected by the system's management and audit methodology." [Gartner Group]*

### 5.7 Desk Top File Encryption

File encryption is another application for an overall secure desktop solution. It allows customer sensitive information to be stored locally on a PC where it is needed; yet the information is safe from prying eyes. There are several file encryption product. All provide the ability to encrypt individual files. Other capabilities provided include the ability to encrypt directories, encrypt entire hard drives, boot protection, and secure deletion. Not all file encryption products utilize public key cryptography; some still rely on symmetric cryptographic techniques.

### 5.8 Wireless Applications (WAP TSL)

The Wireless Application Protocol (WAP) specification from the wireless community provides a single, open architecture and set of protocols to implement wireless Internet access. It is expected that the WAP-enabled applications will revolutionize business processes by allowing immediate access from anywhere geographically, making companies more competitive and responsive.

WAP empowers mobile users of wireless devices to access interactive information services and applications through the screens of mobile phones. Services and applications include email, customer care, call management, unified messaging, weather and traffic alerts, news, sports and information services, electronic commerce transactions and banking services, online address book and directory services, as well as corporate intranet applications.

Wireless IP provides a method to get vital data and applications out in real time to users without having to boot up their laptops. The rise of wireless communications has evidenced the proliferation of WAP enabled devices, service and content providers, network operators and infrastructure providers in support of e-commerce.

Access to the Internet through wireless devices are constrained by processing power, battery life, storage and display capabilities, and simple user interfaces.

To overcome shortcomings in content, WAP has defined an XML syntax called Wireless Markup Language (WML) which optimizes content to suit the limitations of wireless devices (compacted displays). All WML content is accessed over the Internet using standard HTTP requests and WML user interface components map onto existing mobile phone user interfaces. WAP servers are used to convert IP traffic to the WML-based format (streamlined web pages) used in mobile devices.

These wireless applications are part of the new enterprise and come with their own security issues to protect corporate assets. A significant risk with a wireless network is eavesdropping. Wireless Transport Layer Security (WTLS) is the security layer within WAP. WTLS, the wireless version of TLS (an equivalent of SSL 3.1), provides a secure network connection session which addresses a long latency, low bandwidth environment. WTLS provides confidentiality, integrity and authentication between a client and a server, most often a web browser and a web server.

PKI provides added benefits of authorization and non-repudiation required for full participation in e-commerce. Strong authentication can verify the identity of the mobile user or server through certificates issued by a trusted third party. PKI services are embedded within WAP applications through the use of WTLS APIs that provide developers easy interfaces to handle certificate, configure security parameters, and initiate and receive WTLS-secured connections.

### 5.9 Document Transfer (EDI)

Electronic Data Interchange/Electronic Funds Transfer (EDI/EFT) provides a set of negotiated document types for the transmission and subsequent presentation of electronic documents within communities of interest. These formats, such as purchase orders and shipping notices, are established jointly by EDI users through long negotiation sessions to become the X12 or EDI for Administration, Commerce and Transport (EDIFACT) standards used by the transportation, manufacturing, grocery, retailing and computer industries. With the rise of EDI, many large corporations, such as Wal-Mart, Mobil and General Motors, have required that their trading partners use EDI documents for certain business transactions.

Extensible Markup Language (XML) is another technology used to code data exchanged over the Internet. Using data descriptor tags, XML provides a structural representation of the data (as opposed to the text) contained on web pages, thereby extending the possibilities for web-based applications based on HTML and scripts. The use of XML will improve web-browsing applications for viewing, filtering, and manipulating information on the Internet. As use of the Internet spreads to more businesses, customer services will eventually migrate from phone lines and storefronts to web sites. XML is strategically placed to facilitate the rise of business internet requirements.

The usefulness of document transfer technologies is improved by security which guarantees authenticity and trustworthiness of the data over the Internet. Cryptographic techniques are generally applicable to providing public-key encryption and certificate-based authentication schemes. Certificate-based authentication provided by integration with a PKI ensures validation to a trusted root. Secure messaging via S/MIME has been used to provide protection of prepared EDI messages across untrusted networks. Inherent within S/MIME is the facility to perform certificate validation. Signed XML (XMLDSIG) is proposed to provide for digital signature and message authentication codes in XML. This is accomplished through the use of XML API's which electronically manipulate XML documents to digitally sign and encrypt outgoing XML documents, and to verify and decrypt incoming XML documents in real time.

### 5.10 SET

*The State of Iowa appears to have no specific plans to require SET support at this time, and thus no requirements are presumed necessary at this time. However, the information below is provided in case SET is required in the future, for example for on-line purchasing of supplies.*

Visa and MasterCard have collaborated to define the Secure Electronic Transaction (SET) specification as an approach for an Internet-based credit card payment system. Using available cryptographic technologies (public key encryption, digital signature and certificates) and established protocols (SHA, RSA, DES and X.509), it provides businesses a secure mechanism to extend into the Internet.

The series of SET protocols are deployed through software that is implemented via four roles/entities in the payment transaction scenario: certificate authorities, payment gateways/acquirers, merchants and cardholders. Each participant in the transaction is authenticated by public key certificates issued by the CA. Digital signatures are used to validate the authenticity of the transaction while encryption is used to provide confidentiality. The Certificate Authorities are run by certified

payment-processing organizations like Visa and MasterCard and its certified member institutions (banks and card issuers).

It is envisioned that the framework operates within a hierarchy of Certificate Authorities. The Root CA issues certificates to brand CAs. Brand CAs in turn issue certificates to end entity CAs which issue certificates to Cardholders, Merchants, and Payment Gateways.

The trust model established provides considerable confidence that the participants have the authority to undertake the transaction. In the SET protocol, certificates are validated by following their signature chains up the hierarchy of trust to the root CA. Optionally, geopolitical CAs may be established to be responsible for issuing certificates to end entity CAs in specific geographic or political areas.
Research has evidenced that momentum is building in the Internet-based electronic bill presentment and payment (EBPP) market. International Data Corporation (IDC) has forecasted that activity will escalate at a 100% compound annual growth rate through 2004.

## 6.0 Summary of Requirements from Interviews

### 6.1 Overview

The following sections summarize by general topic the requirements, observations, and desired PKI features as provided by interviews with several state agencies. A list of interviewees and their agencies, current responsibilities, and systems that might require PKI with certificates in the future is provided in Appendix 1. Because many requirements were the same for most or all agencies, those requirements are generally discussed but not identified as to source. Where there is a significant difference of opinion about requirements, for example due to different agencies' responsibilities and systems, further information is provided. In general, if even a single agency has a reasonable requirement that could be met without too much trouble by CA vendors, the requirement is included here. Some requirements are more critical than others, as noted in the text, so the less-important requirements might just be considered optional but not essential.

Three topics – certificate format, authentication and CA facility -- are important enough to have their own major section, and thus are covered separately in sections 7, 8 and 9.

### 6.2 Possible PKI-enabled Applications

The following types of applications were identified by at least one interviewee as being of interest. (See Appendix 1 for brief specifics on each agency's plans.) They are listed in approximate order of interest, most popular first.

**Access control**: Essentially all interviewees assumed that the major application requiring certificates would be ensuring proper access control to web-based services for the public or to state employees. This is probably because the new electronic commerce state law mandates that services that now require paper and physical signatures must generally be offered over the Internet, and specifies that digital signatures (defined to apply to RSA or similar signature algorithms) must be used. Digital signatures require certificates, which in turn require a certification authority. Therefore the PKI system must support the use of digital certificates to mediate access to state services provided over the World Wide Web, and allow the services offered to be individually tailored to the individual. This can be done in conjunction with third party products which have a proven interface to the PKI system. Individual tailoring could determined at least in part by the type and content of the individual's digital certificate (or it could be determined by the information in a secure database under that individual's name). Thus, for example, a doctor might be allowed to see medical information but not accounting data, while a CPA might be allowed to see accounting data but not medical data.

**Browsers and web servers**: Several interviewees felt that certificates should protect browsers' and web servers' communications via standard digital certificates. This might be done as part of or in association with the access control function described above. The standard algorithm for protecting such communication sessions is the Secure Sockets Layer (SSL) protocol. Therefore, the PKI system should support and provide SSL certificates for both browsers and web servers. Some applications might use plug-ins to add functionality to browsers, but still look like normal browsers to their CA interface, which allows customized application processing without a need to customize the CA. Note that if the State wishes to provide web

server certificates, a higher standard of authentication than for browsers might be appropriate. Most agencies use Microsoft or Netscape browsers and servers, but at least one agency (Iowa Workforce Development) uses Lotus Domino servers.

**Secure e-mail**: Several interviewees expressed interest in certificate-based secure e-mail, once it was explained how that works. However, in the absence of a mandate requiring this service, they felt that a business case might be needed to decide if secure e-mail is required and what kind of PKI would support it. The standard algorithm for securing e-mail over the Internet is the Secure Multipurpose Internet Mail Extensions (S/MIME). It would be reasonable to require that the PKI system must support the use of digital certificates for secure S/MIME e-mail, which allows both signing and encryption of the e-mail body and attachments. The e-mail packages that are used now, and that should thus be supported if possible, include:

- Microsoft Exchange and Outlook
- Lotus Notes and Groupwise
- Netscape Communicator (Messenger)
- Eudora

**Virtual Private Network (VPN)**: There appear to be no State-wide plans for a secure VPN that would be protected immediately by certificates of the CA planned by ITD. However, the VPN market is rapidly maturing, based on the recently-finalized Internet Protocol Security (IPSec) standard, so it might be wise to include at least an optional requirement that the PKI system be able to support common VPN vendors' products by providing IPSec certificates to routers and firewalls.

**Signing and encryption of files and forms**: A few interviewees also said there might be a use for certificate-based security for exchanging files and providing web forms. This could consist of having the originators of files be able to sign and encrypt the files, so the recipient can be assured who sent them and that they were not altered or examined in transit. Note that the normal SSL protocol discussed above protects files in transit between the sender and the recipient (browser or server, in either direction), so additional protection is probably needed unless files must be stored for some time on a platform that is not fully trusted, which is not normally the case. Similarly, additional protection for web forms submitted to the State, beyond that provided by the normal SSL protection, may be useful. Because the need for such additional protection is not obvious, it might be best to include an optional requirement that the PKI system be able to support certificate-based file signing and encryption, and web forms encryption, but not to make it an absolute requirement.

**EDI and XML**: Rich Varn, the new State CIO, expressed interest in support for the EXtensible Markup Language (XML), which is similar to the HTML language/protocol used for web pages but can be extended to create new variants for a specific application. XML is one of the major ways the Electronic Data Interchange (EDI) is mediated. Therefore it might be prudent to include at least an optional requirement that the PKI system be able to support certificate-based signing and encryption of XML documents. (Also see section 5.9.)

It should be possible to have one certificate perform multiple functions, so users will not have to obtain many certificates. Access control, browser, e-mail, and

sometimes VPN functions have been supported by a single certificate.

### 6.3 Number of Certificates

No interviewees were willing to project how many certificates might be required, since the planning for Internet-based PKI-enabled services is still in the early stages. However, a rough idea of the number of certificates a PKI system might be required to handle can be based on the following estimates, provided by ITD or the interviewees:

- Iowa citizens: 2,800,000
- Citizens employed: 1,500,000
- State and local government employees covered by IPERS (State retirement system): 300,000, including 65,000 getting a State pension
- Licenses or permits of various types: 10,000 liquor licenses, well over 10,000 environmental construction permits
- Number of students and staff in 3 State universities: Close to 100,000
- Percentage of citizens with Internet access: 43%

Given these numbers, a rough guess of the number of certificates that might be required is postulated below, for discussion. CAs could be required to support at least this many certificates annually. ITD can of course modify these requirements.

- Short term (2001-2002): 3 systems with 10,000 certificates and 10 systems with 1,000 certificates.
- Longer term (2003, particularly after 1 July deadline for providing State services via the Internet): 5 systems with 100,000 certificates and 20 systems with 10,000 certificates

### 6.4 Trust Hierarchy

ITD and all interviewees with an opinion agreed that it would be prudent to have at least two levels of CAs: a Root CA which is kept off-line and used only to provide certificates for other CAs, and multiple subordinate CAs that are normally on-line (via the Internet) and providing certificates for end users. The subordinate CAs can be on separate or shared computers, depending partly on the design of different PKI vendors' products, and may be located in one or more secure facilities. It appears that the State of Iowa will want to have its own Root CA, whether operated by a State agency such as ITD or by a service vendor.

Root CAs are normally self-signed: the Issuer (CA) and the Subject Distinguished Name structures are identical. However, the State might be interested in considering having a version of its Root CA that is certified by a commercial CA Root, such as Baltimore Technology's OmniRoot, whose certificate is pre-embedded in common applications. This option is discussed in detail in the next section.

The State may also wish to run one or more X.500 directories with Lightweight Directory Access Protocol (LDAP) interfaces to the CA, which is the industry standard, to hold certificates and certificate revocation lists (CRLs) in a convenient location. Such directories are normally separate from the CA, but all CAs can interface to them. (CAs generally also have their own internal databases, usually Oracle, but these are not intended for direct access by users.)

A simple sample hierarchy showing the above elements and their interfaces is shown below (please view in Page Layout mode if reading a soft copy of this document).

There may also be a requirement for cross-certification with other states and the Federal government. In this case, the State of Iowa CA might wish to have its root be signed by other states/federal agencies, and vice versa. This could allow certificates for one state/federal system to be recognized by another. ITD should consider a requirement that the PKI system be able to support such cross-certification, preferably by exchanging industry-standard PKCS#10 certificate requests with other CAs.

### 6.5 Roots

It is possible that the State of Iowa PKI may not want to chain only to a State of Iowa Root CA. An example is in the web server certificate market; similar arguments apply to other types of PKI enabled applications. All businesses servers or web servers used today are supplied by well known vendors like Microsoft or Netscape. The SSL protocol, described earlier in this report, is what is used to secure connections to these servers. Some PKI vendors like Baltimore Technologies have relationships already established with these vendors and have embedded, within the server and browser products, Root CA certificates. This is done to provide an apparent seamless secure connections to end users. If these root certificates are not already embedded in these products, end users are presented with pop-up warning messages that indicate that the browser or server does not recognize the certificate and it is up to the end user to trust the secured connection. These messages often confuse the end user and they may terminate the connection out of fear of the unknown.

Based on this issue and the desire for the PKI to be easy to use for the end user, Professional Services is recommending that the State of Iowa at least consider chaining up to one of these embedded roots, such as Baltimore's OmniRoot Certificate. This root is already embedded in the server and browser products and will offer less confusion to end users. A possible drawback from the state's point of view is that this may appear to imply a lack of control of the Root CA, although in actuality this is just a technical link and the state will still have and retain control of its "root", even if it is not a true self-signed root. A compromise might to have two "roots" with the same key pair, one a true self-signed root and the other signed by OmniRoot or equivalent, and use whichever is most suitable for a given application.

### 6.6 Certificate Period and Renewal

There was general agreement that certificates should be good for at least the one-year period that is common in commercial applications, and probably considerably longer. The certificate period is generally driven by two considerations: the likelihood of certificate contents changing and the need to obtain revenue. Because the State is expected to have relatively simple certificates and rely on servers to provide other data (this is discussed in Section 7.2), and is not expected to seek revenue greater than expenses at most, a longer certificate period seems reasonable. A typical requirement might be for certificates to be valid for 2 to 5 years, or some systems might best have the certificates synchronized with a license such as a drivers license.

### 6.7 Certificate Revocation

Interviewees generally did not have strong opinions on the process for revoking certificates, so it would be best if ITD could remain somewhat flexible in its requirements for the time being. For reference, the types of issues and options that arise include:

- Who is authorized to request a revocation: the certificate user, an RA, the CA operators, and/or other authorized persons who know the users.
- What verification of the request is done: fax, letter, phone follow-up, e-mail, etc.
- How soon is a new CRL with the new revocation issued: immediately, on a regular schedule, or selectable by an RA or a CA operator.
- The reason for revocation, chosen from a preset brief list, should be saved in an internal CA database, and can be included in the CRL.
- The use of temporary reversible revocation is recommended for consideration. This is variously known as a certificate suspension or hold. If a CRL is issued while the certificate is suspended, it will generally be included in the CRL, but if the suspension is reversed the certificate can be used as normal.

Note that it might not even by necessary to revoke certificates for some systems if a central server database is maintained, as is true for most State web-enabled functions that are planned. Instead, the server can simply refuse to process a user, even if a valid certificate if presented, if it is known that the user is no longer entitled to be served. This is how the SET credit card Internet purchasing protocol cuts off users; there is no revocation for regular users.

### 6.8 Encryption Certificates

Some interviewees thought that it might be a good idea to include the option for separate certificates for encryption keys, as opposed to signing key certificates. There are often good reasons for such a policy: encryption keys are used under different circumstances than signing keys, and might have to be backed up so data can be recovered if the certificate holder becomes unavailable. (Signature keys can not be backed up without risking the legal viability of the individual's signature, and in any case new signature keys can always be used. Recall that signature verification uses the sender's public key, while decryption requires the recipient's private key.)

However, after further discussion it became clear that at least some of the interviewees did not realize that standard SSL web or S/MIME email signature certificates are also used to exchange temporary keys that encrypt data in transit from the sender to the secure State server. (In fact, to have data encrypted it is not even necessary that the browser have a certificate, as long as the web server has an SSL certificate.) Thus the only case where separate encryption keys might be needed is for persistent storage of data in non-secure environments, not a common requirement. However, it is still recommended that ITD require the PKI system to support separate encryption key certificates since there might be a need, and all major CAs already can support this requirement.

### 6.9 Communications Capacity

ITD staff, and other interviewees with knowledge of the State of Iowa backbone and related communications systems, agreed that the State's communications systems are robust and should be able to handle the added traffic for the State CA. Note that a CA is not a major generator of traffic, since a certificate is only required once a year or less often, and generates less than 100 Kbytes of web data and about 10 Kbytes of certificate-related data for the database. Therefore ITD should not have to require any increase in communications capacity due to the PKI system.

### 6.10 Reports

A typical CA supports a set of summary reports that include a listing of the number of certificates of each type, and a one-line summary of the key facts about each certificate or certificate request (e.g., the subject and issuer common names, validity dates, when issued or requested, and the disposition of the certificate request). When asked if that was sufficient information, considering that a directory can provide the full certificate or the CA operator can access the internal database, all interviewees agreed that such reports should be adequate. Therefore ITD may wish to just require such a level of reporting to the CA operators or RAs.

### 6.11 Billing

It is not clear how to charge users for their certificates. In fact, for some systems it is possible the State or an organization to which the user belongs might bear the cost as a service. If users are to be charged for their certificates, common industry billing practices include the following:

- For face-to-face authentication (discussed in section 8), the requestor can pay the authenticator, who in turn informs the CA or RA that payment was made.
- For electronic certificate requests, the user can be billed using a standard "shopping cart" program incorporated into the certificate request application. This might be done prior to contacting the CA's web page, so the CA software need not be modified significantly.
- The user can be billed by mail after the certificate is downloaded. This works best when a centralized server, as is used for most State systems accessed by users, can cut off any users who do not pay.

### 6.12 Help Desk

There was some difference of opinion among interviewees as to how help desk functions should be organized. This difference is legitimate, based on differences in various agencies' existing help desk functions and ability to handle new issues, and the extent to which they control the data needed to satisfy help inquiries. The introduction of web-based PKI-enabled systems with certificates will generate some new help desk traffic, which could be handled by existing agencies' help desks, by a CA help desk, or perhaps some other mechanism. Some thought that their existing help desk should take on questions about browsers, certificates, etc. Others (most interviewees) wanted ITD or the CA operations organization to handle such calls. This matter can be settled in the coming year or more; it does not significantly impact the requirements placed on PKI and CA vendors. However, if CA service providers are considered, they should be required to show that they can provide help desk support at least for PKI and certificate related questions.

### 6.13 Backup Facility

There are no specific plans for a backup facility in case the main CA is incapacitated for some time. However, if such a backup facility is ever anticipated, all agreed that the STARC Armory in Johnston appears to be a good choice, given its preparation as an emergency center and the unlikelihood of a statewide disaster affecting both locations. Note that a CA is not mission-critical in the usual sense, because existing certificates are be used without involving the CA; an incapacitated CA only means that new users cannot be registered.

## 7.0 Certificate Types and Content

### 7.1 Types of Certificates

Multiple different types of certificates may be needed for the State of Iowa PKI. These include:

- SSL certificates for browsers (SSL client certificates), also often used for access control
- Web server certificates (SSL server certificates)
- S/MIME certificates for secure e-mail
- VPN (IPSec) certificates for remote network access
- WAP (wireless) certificates as a possible future requirement
- Encryption certificates, as distinct from signing-only certificates

While each of these is an X.509 certificate they do have different items included in the certificate format. It is often possible to have on certificate format that is accepted by multiple applications, for example one certificate can be used for S/MIME e-mail and SSL browser functions. To the extent this is possible, it will be reflected in the upcoming architecture document.

Appendix 2 provides some examples of what the Server and SMIME certificates might look like. Note these are just examples and the format will change as the architecture is defined. In particular, State of Iowa certificates may be slightly simpler than these examples, for reasons shown in the next paragraph.

### 7.2 Certificate Contents

The State of Iowa certificates can and should be kept as simple as possible. Any data that is lengthy or that is likely to change can be stored in the centralized databases that all State agencies reporting having. Therefore the certificates are used primarily only to establish the unique identity of a citizen or government employee, and can contain a relatively simple Subject Distinguished Name and Issuer Distinguished Name, and a few extensions that are recommended for the applications that are expected to rely on these certificates. A more detailed analysis will be provided in the upcoming architecture document to be delivered under this consulting contract, but the following guidelines appeared reasonable to those interviewees who felt competent to discuss the issue:

- Subject Distinguished Name:
  - Country, State: US and Iowa respectively.
  - Organization: State of Iowa or equivalent.
  - Organizational Unit: Organization (state agency, licensed body, company, etc. as appropriate) only for certificates that are intended to be used only in the individual's capacity as a member of the organization.
  - Common Name: The individual's normally-used name, e.g. John Q. Smith.
  - Date of Birth: To be used to distinguish cases of individuals with identical names.
  - Other information, if needed (but should be avoided otherwise), such as address, phone number, or student ID number.

- Issuer Distinguished Name:
  - Country, State: US and Iowa respectively.
  - Organization: State of Iowa or equivalent.
  - Common Name: State of Iowa Certification Authority or equivalent. (For subordinate CAs, specify the system that uses that CA.)

- Common extensions:
  - Subject Alternative Name: for e-mail address, IP address (for VPNs), and ultimately possibly EDI name or other identifiers.
  - Various other possibilities to be examined further in the architecture document.

## 8.0 Registration Processes

### 8.1 Levels of Authentication

ITD suggested that the State offer multiple levels of certificates, with varying levels of authentication effort to match the security of the certificates and the systems they protect. Essentially all interviewees agreed that this would be a good idea. At least three possible approaches were considered, each of which were tentatively endorsed by multiple interviewees for at least some of their systems. These are summarized below, and discussed in more detail in the following sections.

- Face-to-face: This is the most secure and flexible alternative. A certificate requestor would appear in person and provide information and documentation required for the particular PKI-enabled system. This is similar to obtaining an initial drivers license. The exact requirements could vary on a case-by-case basis, within broad guidelines.
- Shared secret: A purely electronic certificate request process can be followed, but the requestor can be required to present a password, numeric code, or other data before the certificate is authorized. This is similar to how America Online hands out CDs with a code that has to be entered to get a free subscription. This password can be provided to the requestor by the CA and/or RA in advance, or can be provided to the CA/RA by the requestor. In either case, it is passed "out of band" by some secure process such as the U.S. mail or by hand. This approach works best when possible users are known to the State in advance.
- Request data only: This is the least secure but most convenient option suggested, and may be adequate for low-to-medium security systems. The requestor contacts the CA, applies for a certificate, and provides whatever data is required. If it is deemed unlikely that the requestor is pretending to be someone else, the RA can approve the request.
- One suggestion by DOT staffers is that the State might want to consider offering a low-level certificate to anyone who has a drivers license or DOT ID card. This could be handled by DOT staff at motor vehicle offices, but not require additional special identification for authorization.

### 8.2 Manual Authentication

One method of conducting registration is a manual (and possibly face to face) method. In the manual model an authorized person at a browser or RA (Registration Authority) station using an SSL-protected connection to the CA, downloads, reviews, and approves end-user certificate requests. The authorized person can refer to any additional records, make phone calls, etc. as required for that system, to be reasonably certain of the requestor's identity and right to obtain a certificate. The requestor typically logs on at a later time to download the certificate.

In one variant of the manual authorization model, the RA will review information from the certificate requestor in person. The requestor may be required to provide supporting documentation, sign papers, or pay a fee at this time. This method is useful for small numbers of users or when high levels of authentication are needed. It becomes too labor intensive when the number of certificates issued exceeds about 1000 users.

### 8.3 Automated Authentication Methods

As the number of users increases, the need for an automated process also increases. Any PKI offering that issuing more than about 1000 certificates to a customer organization may require a labor force that the agency cannot support.

Two example methods for an automated process follow.

In the first case, a Pre-Authorized list of users along with a file containing authentication data is provided to the CA, in advance, by the user's organization. As requests are received electronically the information in the file is compared against certificate request data so that approved certificates can be provided immediately to the user. This method is usually sufficient for volumes up to 10,000 certificates. After this point the information in the file becomes too difficult to manage.

If the number of certificates to be issued exceeds 10,000, then one could realistically assume that an organization of this size would already have user information in an existing database. In this case a connection can be made between the CA and the organization's database. This is essentially an automated equivalent to an RA, where instead of a person at a browser, the authentication is performed by a program that interfaces between a protocol at the CA and a customer back end system or database.

### 8.4 Authentication Criteria

The exact data required in a certificate request will depend on the particular PKI-enabled system and the preferences of the state agency that controls that system. In addition to the personal data that goes into a certificate, there was general agreement that the following data might be good candidates for authentication purposes, and the CA should be required to support them:

- Social Security Number (SSN): This is the one universal unique identifier for most U.S. citizens. All interviewees expressing an opinion thought it is appropriate for inclusion in the certificate request and system database. However, all also agreed that the SSN is not suitable for inclusion in the certificate itself, due to privacy laws.
- Drivers license number. (This might be a substitute for the SSN in some cases, if the two numbers differ.)
- Date of birth
- Address, phone number, e-mail address, etc.
- Other data commonly used by credit card companies, etc., such as mother's maiden name, place of birth, etc.
- A shared secret (PIN or password), chosen in advance by the user and communicated to the CA/RA or vice versa.
- Identification of organizations such as companies or agencies, for certificates granted only for use by the individual as a representative of that organization. Details will unfortunately vary, as there is no single identifier for organizations similar to the Social Security Number for individuals.
- Paper documents, such as a drivers license, corporate papers, etc.: These would be used only in a face-to-face environment, and requirments could be set aside from any CA or RA operational considerations.

### 8.5 Who Performs Face-to-Face Authentication

One difficult issue is deciding who will perform face-to-face authentication as part of the certificate request issue. A logical entity might be the Department of Transportation's motor vehicle offices, which are already in every community. The DOT is also already in the identification business, because drivers licenses or equivalent ID cards are already a widely accepted standard for identification. Unfortunately, the DOT expressed no interest in taking on this role for any systems outside their core business areas. Interviewees were unable to think of another equivalent organization, in their own agencies or elsewhere, that could easily serve this function.

One possibility might be that some existing notary publics could be trained to perform face-to-face authentication and use the Internet via a web browser to report results. However, almost all interviewees felt that notaries are not sufficiently screened and reliable enough to be given this task, at least for very sensitive systems, and did not recommend that this option be pursued further.

### 8.6 Who Performs RA Functions

Interviewees' opinions varied about who should act as a Registration Authority for a given system. Some agencies are likely to want to act as the RA for their own systems. This is more likely the case when an agency has its own tightly controlled database with little interaction with other agencies, and has a tradition of performing its own authorization. Examples are the State personnel and retirement plan (IPERS) systems or state universities (with registrar offices as RAs). Other agencies may have extensive contacts with outside organizations and might not have easy access to all data needed for registration. In this case it might make more sense to have a more centralized shared RA, perhaps even an RA function contracted out to a service vendor. In fact, it may make sense to have the agencies share a single CA as well. Examples might be some DOT functions or Public Safety (law enforcement). This issue is something the State will have to decide on a case-by-case basis. It has little or no impact on the CA, however, since CAs should be required to support remote RAs at any location.

### 8.7 PKI Kiosks

One suggestion from ITS, which a few interviewees thought might be useful, is to offer kiosks for some systems, whereby certificates requestors could come to a central location and obtain a certificate there. The kiosk might be manned by a PKI-trained State employee, who could help the requestor, and possibly also act as a face-to-face authenticator and/or RA. Once the information has been validated the RA can help the requestor generate key pairs and the certificate. The certificates thus obtained could either be put into a PKCS#12 floppy disk file or a smart card and taken to the requestor's own PC. Alternatively, the certificate might be installed and used on the spot at the kiosk to access the PKI-enabled application. In the latter case, a very short-lifetime certificate (e.g., one hour or one transaction session) might be used, and no revocation would be necessary.

Note that the RA must not make copies of the keys, and should not observe any PIN entry if possible, to ensure that the requestor's private key security is maintained for legal reasons.

### 8.8 Biometrics

Rich Varn, the new State CIO, expressed an interest in the ultimate use of biometrics to provide unique identification. This might be used in concert with digital certificates in the future. ITD may wish to require that prospective CA vendors suggest ways to use biometrics with certificates, perhaps including the biometric "indicia" (compressed biometric measurement data) in the certificate itself. It should be noted that despite some discussion of this issue in the biometric and PKI industries, there is no standard or even informal consensus as to exactly how this should be done.

### 8.9 Data Sensitivity

Many State systems handle very sensitive data, for example medical records, financial information, arrest records, etc. This must generally be carefully protected according to legal practice or government regulations. However, the sensitivity level for data used in the certificate request process is considerably less sensitive than this. Therefore it is not necessary to be unusually aggressive in controlling who sees certificate request data. The data in the certificates themselves is not at all sensitive, since certificates are essentially public records.

## 9.0 CA Hosting Facility

### 9.1 Facility Overview

The following sections cover requirements necessary to ensure a location is at a security level appropriate for a CA. They describe physical security equipment and procedures which should be followed when accessing the facility, and summarize staff members that might be required. If a commercial CA is used as an outsourced CA, these requirements should be placed on the CA, since they follow accepted current standards for a secure CA facility. If the State of Iowa chooses to run its own CA using vendor hardware and software, similar facility requirements are suggested, but the State can decide which requirements to apply as long as no formal facility approval is required (e.g., by a state agency, credit card company, etc.).

## 9.2 CA Facility Security Requirements

### 9.2.1 Introduction

We suggest that a secure facility suitable for hosting the State of Iowa should meet the following requirements. Those that are already met by the ITD facility in the Hoover Building, which would be a likely facility if the State of Iowa runs its own CA, are so noted. Other requirements would have to be met by enhancing the current State facility's physical security, operations, or equipment as appropriate. Facility staff requirements are covered separately in section 9.3.

(It might be appropriate to examine the STARC Armory in Johnston IA to see if it would be suitable for hosting a CA facility. As this is not in Des Moines, it was not visited during the interview / site visit trip.)

These requirements should be specified for any commercial CA hosting facility if an outsourced CA is planned. Most requirements are already met by existing CAs, and any significant reduction in capability would not be considered good PKI practice.

### 9.2.2 Site Physical Security

The site that contains the CA facility should be in a controlled building, with lockable doors and an entry guard able to screen visitors and handle emergency situations. The CA facility itself should have separate locked doors and require a special access swipe card or equivalent. These requirements appear to be met for the Hoover Building site, and should be required of any commercial outsourced CA facility that might be used.

Some additional requirements are mostly not met in the Hoover Building, and would require additional construction or equipment installation. These include:

- A separate secure room for the offline Root CA, and a different room for the online Subordinate CAs. These rooms should be "sealed" to the extent that it is not possible to crawl into them via a false ceiling or floor or a ventilation duct. Steel-mesh reinforced walls and solid-core doors are recommended, so an intruder needs something more than a simple knife to get into a room. A separate room for CA-related communications equipment such as routers, firewalls, and web servers is also recommended. Support functions such as CA operator stations or network monitoring can be performed in a general room with normal security. The State could use locked cabinets instead, although this is not recommended, but outsourced CA service providers should be held

to this requirement.

- Special controls for these CA secure rooms, including door locks connected to one or more of the following access controls: special-access swipe card readers or equivalent, cameras with video tapes, motion detectors, and alarms.
- Two-person control for the CA is recommended, similar to that typically required for banking and credit card CA operations. This means that the door opening logic requires two authorized card swipes, or equivalent protection, before a secure room can be entered. The State can drop this requirement if it runs its own CA and is willing to assume the risk, but any outsourced CA should be required to provide two-person CA room control.
- Biometric devices such as fingerprint readers can be used to augment other physical security checks and to more surely identify individuals. This is not always a CA requirement, but is good practice, and also good marketing to show off the facility security. Most CAs have biometric readers today.
- Automatic logging should be required to keep auditable records of physical security devices, alarms, unusual computer hardware or software events, and CA operational abnormalities.
- An requirement that is recommended, at least for outsourced CAs, is redundancy of all equipment that is likely to fail. Equipment could be duplicated to run in parallel (this works well for web servers or subordinate CA workstations), or could be pre-installed spares ready to switch over to replace a failed unit's functions within a few minutes.

**9.2.3 Facility Operational Controls**

A CA facility should meet the following operational control requirements:

- The CA facility should have well-document security policies and procedures documents, describing how security requirements such as those summarized here are met, and should be communicated to all new employees and reiterated periodically for existing staff members.
- The facility should also have plans documented for handling emergencies (e.g., fire or medical), area-wide disasters (storms, and earthquakes if in a seismically active zone), and "incidents" (possible intrusion attempts or attacks via the Internet that could lead to a compromise of facility security).
- Operational enforcement of two-person access controls should be required, to reinforce and enhance the two-person logical controls discussed in the section above.
- Controls should be required to control passwords and PINs, media security controls (e.g., document classification and destruction), audit record management, and personnel records.
- Regular audits (weekly or at least monthly) should be performed to determine if operations are proceeding normally, and to investigate any suspicious events. These audits should cover paper logs (sign-in sheets and safe opening records), physical security device logs (cameras, motion detectors, etc.). The audits should also research current threats, as reported by security industry watchdog groups, to determine if any changes to security practices are needed.

## 9.3 CA Facility Staff

### 9.3.1 Required Personnel

Hosting a CA requires the need for several personnel. It requires technically skilled people, management, and security personnel, as well as sales and marketing types.

Based on other CA Hosting facilities throughout the world and with in Baltimore Technologies, Professional Services is suggesting the following staffing requirements, assuming a 24 x 7 facility is required. (If fewer staff are used, the CA might have to shut down occasionally if problems occur over night, or facility security might be impacted somewhat.)

- A minimum of 5 full time CA Staff
- 2 part time staff (equaling a 1/2 full time person)
- 1 or 2 sales and market staff and 1 technical sales support person.

These numbers could grow as the state's online business also grows.

Following sections describe representative CA staff and tasks they perform.

### 9.3.2 Staff and Responsibilities

This section lists typical staff members by role, and responsibilities for each role. Some roles may filled by multiple individuals, and some individuals may have multiple roles. Others roles may be filled by only one person, although routine duties may be delegated to other staff members with the permission of the responsible staff member. Such delegation, or other changes in responsibilities, should be documented in writing if they could impact the security of the CA facility.

### 9.3.3 Officers

Officers are officials of the State or its customers, but not CA facility personnel, who are called upon to represent the CA in special circumstances. There are two types of corporate representatives.

- Key Control: Officers control components needed to create cryptographic keys and certificates. For example, a Root CA key is normally under the control of officers outside the CA, to guard against internal attacks on the CA. The Officers hold the combination for the inner safe that holds the Root CA cryptographic card. These Officers must be brought together with CA staff members to create the high-level CA keys and certificates that are used to sign the regular operational subordinate CA and end user certificates.

- Point of Contact (POC): Other Officers (or the same people in some cases) may act as a point of contact to the outside world, particularly in unusual circumstances such as disasters, security incidents, or other problems. This has two beneficial effects: it ensures that the state presents consistent information to the public, press, or interested organizations, and it frees the CA staff to solve the problem. Depending on the nature of the situation, these POCs may be lawyers, public relations experts, or business experts.

**9.3.4 Facility Manager**

The Facility Manager, sometimes called the Site Manager, is the single facility officer in overall charge of the facility. Duties include:

- Assigning other staff members' roles, and authorizing exceptions such as acting roles or multiple roles for one person.
- Approving facility operational policy and security policy, and any significant changes
- Approving the facility hardware, software, and configuration, and any significant changes
- Approving staff members' privileges for access to CA components. This includes determining who shall be given passwords (particularly UNIX root or Database Administrator passwords), cryptographic cards with their PINs, or other items necessary to access sensitive components of the CA facility.
- Verifying the physical security of the CA facility by directing periodic checking and holding audit logs
- Notifying customers of possible shutdowns or changes in operations
- Participate in teams for dealing with all responses to disasters or security incidents
- Ensuring that a reasonable schedule is maintained for renewing CA keys and certificates
- Generally making sure the facility operates as intended

*Notes:*
*There is some flexibility in determining what is done by the Facility Manager, and what by the Site Security Officer. Their roles may depend partly on how familiar the Facility Manager is with day-to-day operations of a networked facility like the CA. A more technically experienced Facility Manager might be involved in the detailed workings of the facility, while a Facility Manager more familiar with policy and business matters may leave more to the Site Security Officer.*

**9.3.5 Site Security Officer**

The Site Security Officer, sometimes called the Site Security Manager, is the facility officer in charge of security matters. The Site Security Officer is the most important individual for ensuring that the Security Procedures are effective, and must generally ensure that security procedures are understood, implemented properly, and followed.

Specific duties of the Site Security Officer include:

- Physical and operational security
- Implement privileges determined by Facility Manager
- Provide specific combinations and passwords to CA staff members approved by the Facility Manager, and keep track of who has which combination or password
- Implement, supervise, and check security measures, including those specified by the Facility Manager
- Review facility security and audit logs
- Perform security audits and reports
- Control UNIX root password (can split and gives halves to others)
- Set up UNIX accounts for Site Administrators
- Participate in teams for dealing with all responses to disasters or security incidents
- Describe facility security measures to auditors or credit card organizations

- Control passwords and smart cards needed to allow Online Operators access to their web page
- Approve any "no authorization" settings for certificate renewal. (Note: the State of Iowa is not expected to allow this setting.)

**9.3.6 Data Base Administrator**

The Data Base Administrator (DBA) is the facility staff member responsible for overall running of the Oracle database. Duties include:

- Controlling the database "root" password
- Making any database changes beyond that resulting from normal CA operation
- Generating custom reports
- Other special database accesses

**9.3.7 Site Administrators**

Site Administrators, also known as System Administrators, are facility staff members responsible for technical matters, including physical access to UNIX workstations and software inside the secure rooms. There can be more than one Site Administrator present at any time, but one Site Administrator is considered to be in charge at any time, e.g. one per shift.

Site Administrator functions include:

- Obtaining HSM devices, PINs, and UNIX passwords when authorized
- "Key cutting" and creating Online CA cryptographic cards (setting up new CA cryptographic signing engines) when directed by Facility Manager
- Setting up, configuring, starting and stopping CA(s)
- Creating certificate revocation lists (CRLs)
- Mirroring or backing up and restoring CA keys
- Renewing CA keys
- Running UNIX utilities
- Arranging for signing of audit logs
- Activities at the workstations that are unusual or complex
- Installation of hardware or software
- Any modification of Perl or shell scripts if needed for CA customization, but only if the Facility Manager approves it and the Site Security Officer reviews the changes for correct functioning
- Limited operations outside the CA rooms by running applications from the System Monitor PC or an Online Operator PC.

**9.3.8 Online Operators**

Online Operators are facility staff members who access the CA outside the CA rooms via web programs, much like customers' Registration Authorities, for example to provide customer service and help desk support. Site Administrators are normally also authorized to perform Online Operator functions. Some Online Operators, may also be allowed to perform some Site Administrator functions inside the secure CA rooms, when authorized by the Facility Manager. There is normally at least one Online Operator present at any time. Online Operator functions can include:

- Customer service and help desk support
- Obtaining Online Operator access control smart cards, PINs, and web page usernames and passwords, when authorized

- Checking the status of certificates or certificate requests when requested
- Approving authorized RAs' requests for certificates
- Revoking users' certificates, when authorized to do so by an agency or user
- Creating and manipulating reports on certificates, certificate requests, or audit summaries
- Approve certificate requests

**9.3.9 RA Operator**

The RA Operators are facility staff who will be responsible for authenticating customer information and approving user certificates. This role applies to the state when for instance issuing Server or WAP certificates directly from the CA. The role of RA will be provided by an agency when certificates are issued by the agency for its employees or customers. RA Operator functions include:

- Customer service and help desk support
- Checking the status of certificates or certificate requests when requested
- Authenticating information collected from customers.
- Revoking users' certificates, when authorized to do so by an agency customer
- Creating and manipulating reports on certificates, certificate requests, or audit summaries
- Approve certificate requests
- Generate customer key pairs (when requested) and loading them on smart cards or floppy disk

**9.3.10 Security Functions**

Security personnel are not part of the facility staff and are not allowed to perform any CA functions. They are responsible for monitoring physical security devices, tracking alarms, providing badges, and responding to building emergencies. The State of Iowa has a security department and it is expected to provide these function:

- Building security: Observing building entrance security, controlling individuals' access to the building outside of normal working hours, and responding to disasters or physical attacks, including calling police or fire departments when needed.
- Remote monitoring of alarms, and checking on the status of the CA facility or building when prudent for certain alarms (fire, breaking glass, etc.)
- State personnel administration: Providing badges of two types: a normal state employee badge, and a special proximity badges used to access the CA facility and (for those authorized) the secure CA rooms.

**9.3.11 Staff Assignments**

The Facility Manager maintains lists of the personnel who fill the various staff positions at the CA facility, with reference to their positions in the CA organization chart. This list must be updated as changes in staff or assignments occur. Each staff member is responsible to perform the duties for that position, as described in the preceding paragraphs.

# Appendix 1 Agency Staff Interviewed and Possible Applications

| Interviewees | Agency | Responsibilities | Possible Future PKI-enabled Systems |
|---|---|---|---|
| | | | |
| Ken Adrian<br>Kip Peters<br>Todd Wouters | Information Technology Department (ITD) | Overall PKI responsibilities (and the point of contact for this consulting engagement), CA facility planning | General support for possible applications listed below.. (Those mentioned by other agencies marked with *).<br>Online versions of current face-to-face / paper systems.*<br>Access control.*<br>PKI kiosk.*<br>Library access.*<br>Drivers license.*<br>Contracts, purchasing, bids.*<br>VPN (ITS).*<br>Professional licensing.*<br>Medical record transfer.*<br>Permits.*<br>Secure e-mail.*<br>Law enforcement records.*<br>Interfaces to other states or Federal, including cross-certification.*<br>Smart cards.*<br>Insurance forms.<br>ERP roadmap, e.g. accounting.<br>Voucher reimbursement. |
| | | | |
| Sharlene Newton | IA Department of Personnel | Run AS400 system shared with IPERS (below) | Job applications.<br>Benefits enrollment/changes. |
| | | | |
| Dan Combs | ITD | Primarily interested in management and policy | No specific new PKI systems discussed. |
| | | | |
| Cheryll Marvin | IPERS (State retirement system) | IPERS core system: employee wage withholding & benefits, employer records | Members' web access to their accounts; e.g. change address or beneficiary, employer verification of records. |
| | | | |

| | | | |
|---|---|---|---|
| Terry Dillenger | Department of Transportation (DOT) | Director of Drivers Services: drivers license, vehicle registration, taxes, trucking, motor vehicle enforcement & investigations | If possible, web versions of all activities listed in box to the left ← |
| | | | |
| Kathy Cullor | ITD | Systems support: desktop support, file servers, etc. | Web-based applications like license renewal.<br>Secure e-mail.<br>Custom applications to be determined. |
| | | | |
| Marty Deaton<br>Lynn Walding<br>Jim Kuhlman<br>Kay Chapman | Department of Commerce | Administration; Alcohol and Beverage Division functions (vendors and retailers); professional licenses | Liquor: license renewal (not original); supplier price quotes; shipper & retailer records.<br>Deeds. |
| | | | |
| Rich Varn | State CIO and head of ITD | Administration, general requirements and technology | Biometrics (perhaps tie-in to PKI).<br>XML. |
| | | | |
| Greg Fay<br>Phyllis Blood<br>Jeff Hoyem | Department of Public Health | Information Management: bureau chief, project manager and database administrator respectively | Secure transmission of medical information among doctors, hospitals, funeral directors, etc.<br>Records: immunization registry, electronic birth certificates. Later: death certificates, professional licensing. |
| | | | |
| Joan Thompson | Iowa State University | ISU Treasurer | Fee payment.<br>Financial aid.<br>Business-to-business forms.<br>Remote access to computer lab software.<br>Library access.<br>Transcripts.<br>Secure e-mail.<br>Interfaces to other agencies. |
| | | | |
| Rich Jacobs<br>Ray Hague | Department of Revenue and Finance | Administration and systems for state taxes and state accounting systems | Online information.<br>EDI for payments & funds transfer. |
| | | | |

| | | | |
|---|---|---|---|
| Larry Grund | Department of Public Safety | Law enforcement information support, including high-security user authentication requirements per Federal regulations | Interaction with FBI per Federal requirements.<br>Online warrants access.<br>Biometrics.<br>Online image access (photos, fingerprints). |
| | | | |
| Sandy Scharf<br>Roel Campos<br>Brian Boyd | Legislative Computer Support Bureau (Legislative branch, not Executive) | Administration (Sandy Scharf is Bureau Director) and systems. | Information support for legislators and staff (only).<br>Ombudsman office.<br>Secure e-mail? |
| | | | |
| Linda Torgeson<br>Charlotte Bentley<br>Roger Rohlf<br>David Beary | Department of Transportation | Administration, database/architecture studies, system programming, and motor vehicle support respectively. | Primarily web renewal or data change for drivers license.<br>Other identification or support functions as mandated. |
| | | | |
| Stan Kuhn | Department of General Services | Purchasing administration, procurement for state agencies | Protect Java-based client/server system.<br>Online payment.<br>Online bids & proposals.<br>Interfaces to other agencies. |
| | | | |
| Liz Murray<br>Cherity Gabrielle<br>Judy Pawell | Department of Natural Resources | Air Quality Bureau applications & support, hunting/fishing licensing, water database | Online environmental user support & permit applications.<br>Online hunting/fishing licensing. |
| | | | |
| Diana Thompson<br>Larry Venenga | Iowa Workforce Development | IT administration/systems, support for unemployment insurance | Online support for public & employers.<br>Service provider (for employers) authentication.<br>Data exchange with other state and Federal agencies.<br>Future: web filing of unemployment claims. |
| | | | |
| George Covert<br>Rich Jones | Iowa State University | Systems and technology including PKI, Federal requirements. | Student access to financial and academic records.<br>Online library access.<br>E-commerce such as credit card transactions (but not SET at this time).<br>Multi-function credit cards.<br>Interfaces to other universities. |
| | | | |

# Appendix 2 Sample Certificate Format

*[This information will be refined and customized for State of Iowa certificates in the follow-on architecture document. Some fields may be dropped.]*

| | SMIME | Device e.g Server | Critical | Type |
|---|---|---|---|---|
| **Version** | 3 | 3 | | Integer |
| **serial number** | [Certificate Serial Number] | [Certificate Serial Number] | | Integer |
| **signature algorithm ID** | md5RSA | md5RSA | | OID & State |
| **issuer name** | CN=State of Iowa CA,<br>OU=State of Iowa,<br>O=SMIME,<br>C=GY | CN=State of Iowa CA,<br>OU=State of Iowa,<br>O=SSL Cert,<br>C=GY | | Name |
| **validity period** | issued date [UtcTime] | issued date [UtcTime] | | UTC Time |
| | 1 year from the issued date [UtcTime] | 1 year from the issued date [UtcTime] | | UTC Time |
| **subject name** | C=GY,<br>O=name of Business,<br>OU=[long name of org unit,<br>OU=[Subscriber Reference Number],<br>CN=[long name of subject],<br>emailAdr=[SMTP email address] | C=GY,<br>O=name of Business,<br>OU=[long name of Dunn and Bradstreet or equivalent,<br>OU=[Subscriber Reference Number],<br>CN=[long name of subject],<br>emailAdr=[SMTP email address] | | |
| **Subject Public key Info** | RSA Algorithm | RSA Algorithm | | Bit String |
| **Issuer Unique Identifier** | Unused | Unused | | |
| **Subject unique identifier** | Unused | Unused | | |
| **Extensions** | see below | see below | | |
| **issuer's signature** | md5RSA | md5RSA | | OID |
| | Certificate Signature | Certificate Signature | | Bit String |
| **Standard Extension** | | | | |
| **Authority Key Identifier** | (Dynamic over time, this field is used to point to the signing CA certificate used for signing this certificate) | (Dynamic over time, this field is used to point to the signing CA certificate used for signing this certificate) | N | |
| | CN=State of Iowa Root Certification Authority,<br>OU=SMIME,<br>O=State of Iowa,<br>C=GY | CN=State of Iowa Root Certification Authority,<br>OU=Server,<br>O=State of Iowa,<br>C=GY | | |
| | Certificate Serial Number | Certificate Serial Number | | Integer |
| **Subject Key Identifier** | Key ID | Key ID | N | |

| | | | | |
|---|---|---|---|---|
| **Key Usage** | DigitalSignature + KeyEncipherment + DataEncipherment | DigitalSignature + KeyEncipherment + DataEncipherment | Y | |
| **Certificate Policies** | Unused in this stage | Unused in this stage | Policy OID | |
| | Policy OID | Policy OID | | OID |
| | CPS - URI | CPS - URI | | URI |
| **Policy Mapping** | Unused | Unused | N | |
| **Subject Alternate Name** | rfc822Name=[SMTP email address] | rfc822Name=[SMTP email address] | | |
| **Issuer Alternate Name** | Present but Unused | Present but Unused | N | |
| **Subject Directory Attributes** | Unused | Unused | N | |
| **Basic Constraint** | (Set to Logical #0) | (Set to Logical #0) | Y | |
| **Extended Key Usage** | Unused | Unused | | |
| **CRL Distribution Points** | [DistributionPointName] | [DistributionPointName] | | |
| | CN=State of Iowa Root Certification Authority, OU=SMIME, O=State of Iowa, C=GY | CN=State of Iowa Root Certification Authority, OU=Server, O=State of Iowa, C=GY | | |
| | CertificateHold+CessationOfOperation+CACompromise+KeyCompromise+AffiliationChanged | CertificateHold+CessationOfOperation+CACompromise+KeyCompromise+AffiliationChanged | | |

# References

**Other Relevant Documents**

- FIPS 140-1
- FIPS 46-3
- FIPS 186
- Gartner Group web-pages
- ISO/IEC 7498-2
- State of Iowa Electronic Commerce bill (now passed into law)